

Snapping up cheap spy tools, nations 'monitoring everyone'

August 2 2016, by Frank Bajak And Jack Gillum



Pedestrians talk on their cellphones in Lima, Peru, on Monday, Aug. 1, 2016. Under a July 2015 decree, police now track cellphone locations without a court order but would need one to listen in. All four Peruvian phone companies are cooperating. They signed a pact with the government in October the details of which were not disclosed. (AP Photo/Martin Mejia)

Governments known to stifle dissent with imprisonment and beatings or otherwise abuse their power are buying cheap, off-the-shelf surveillance

software that can monitor the phone conversations and track the movements of thousands of their citizens, an Associated Press investigation has found.

Such so-called "lawful intercept" software has been available for years to Western police and spy agencies and is now easily obtained by governments that routinely violate basic rights—outside a short blacklist that includes Syria and North Korea. For less than the price of a military helicopter, a country with little technical know-how can buy powerful surveillance gear.

Domestic spy operations rely upon companies like the Israeli-American firm Verint Systems, which has customers in more than 180 countries. Verint has also supplied U.S. law-enforcement agencies, including those that target drug traffickers in Mexico and Colombia.

The scope and sophistication of Verint's products is made clear in confidential documents obtained by The Associated Press in Peru. They mirror on a small scale U.S. and British surveillance programs catalogued in 2013 that showed how the U.S. government collected phone records of millions not suspected of any crime.

The documents, including training manuals, contracts, invoices and emails, expose in greater detail than previously seen the inner workings of a highly secretive industry. Verint, and companies like it, disclose little about their surveillance products and who buys them.



This Thursday, July 28, 2016 photo shows the Verint offices in Herzliya, Israel. The Mellville, N.Y.-based company discloses little about its surveillance products, which it says collect and parse massive data sets to "detect, investigate and neutralize threats." Such so-called "lawful intercept" software available for years to Western police and spy agencies is now easily obtained by governments that routinely violate basic rights. (AP Photo/Dan Balilty)

In Peru, the nation's domestic intelligence agency spent a mere \$22 million on a Verint package just months before its activities ground to a halt in a domestic spying scandal. The AP independently confirmed sales in countries including Australia, Brazil, Mexico and Colombia.

"The status quo is completely unacceptable," said Marietje Schaake, a European Union lawmaker pushing for greater oversight. "The fact that this market is almost completely unregulated is very disturbing."

Analysts say about half of Verint's surveillance dealings are in the

developing world. Since the early 2000s, Verint and top competitor Nice Systems have sold mass surveillance products to the secret police in Uzbekistan and to Kazakhstan, the advocacy group Privacy International has reported.

That equipment has let Uzbek police quickly locate and arrest people who discuss sensitive information on the phone or via email, dissidents say. "The authorities' main weapon is people's fear," said Tulkin Karayev, a Sweden-based exile. "Freedom of speech, freedom of expression—all this is banned."



This Thursday, July 28, 2016 photo shows the Verint offices in Herzliya, Israel. The Mellville, N.Y.-based company discloses little about its surveillance products, which it says collect and parse massive data sets to "detect, investigate and neutralize threats." Such so-called "lawful intercept" software available for years to Western police and spy agencies is now easily obtained by governments that routinely violate basic rights. (AP Photo/Dan Balilty)

Verint declined to comment for this story, saying it rarely speaks with reporters. Asked whether Nice Systems' sales had enabled political repression, the spokeswoman for Ebit Systems, which bought it last year, declined to comment. "We follow the leading standards of corporate governance and focus on ethical behavior in our business dealings," Dalia Rosen said.

Spyware installations are a good business, requiring constant updates to keep up with the latest technologies. And they can easily outlast governments.

Take the Caribbean nation of Trinidad and Tobago, whose government fell after a wiretapping scandal involving Verint-supplied equipment. In that case, 53 people, including politicians and journalists, were illegally monitored. Yet the Verint platform remains operative.

As in Trinidad and Tobago now, most countries require a judge's sign-off to use the technology. But where the rule of law is weak, abuse is not uncommon.



This image shows a page from a Peruvian government document dated August 2015, obtained by The Associated Press. It outlines a domestic electronic surveillance platform from the American-Israeli firm Verint Systems. This page shows a photo of buildings in Peru's capital, Lima, where it was being installed; labels indicate offices for prosecutors, meeting rooms and "listening rooms." Originally acquired by Peru's intelligence agency, the platform is now to be staffed by police. (AP Photo)

One apparent spyware client is the government of South Sudan, where a 2 1/2-year-old civil war has claimed tens of thousands of lives. The United Nations and human rights groups say the government has used surveillance tools from Israel to track down, jail and torture dissidents and journalists.

The U.N. experts who pointed the finger at Israel did not name the

Israeli supplier and a government spokesman refused to discuss the issue, though an AP reporter did identify two Verint employees in May on a flight from Ethiopia to the South Sudanese capital of Juba. Human rights activists say heightened surveillance there has fostered a climate of fear and self-censorship.

What regulations exist in the commercial, mass-surveillance trade fall under a non-binding international arms-export-control regime called the Wassenaar Arrangement. In December 2013, it was amended to add two categories of surveillance tools: monitoring products and intrusion software, which surreptitiously turns digital devices into remote listening posts. The United States has yet to ratify the amendment, although the European Union has.

Victims of these surveillance tools report being confronted by their eavesdropped emails and conversations.



New Interior Minister Carlos Basombrio, foreground, and Finance Minister Alfredo Thorne attend the inauguration ceremony for President Pedro Pablo Kuczynski at Congress in Lima, Peru, on Thursday, July 28, 2016. Three years after its acquisition, the Verint surveillance system purchased by Peru has been installed but is not up and running, says Basombrio. "When it becomes operative, it will be used against organized crime, with judicial oversight." (AP Photo/Martin Mejia)

Joseph Bakosoro, a former South Sudanese state governor held without charge for four months this year, said his interrogators played for him a

voicemail that had been left on his cellphone, claiming it as evidence he backed rebels.

Baksono said the voicemail proved only that he was being wiretapped.

"They told me they are monitoring me," he said. "They are monitoring my phone, and they are monitoring everyone, so whatever we say on the telephone, they are monitoring."



This undated photo provided by exiled Uzbek activist Tulkin Karayev shows

dissident Kudrat Rasulov, a blogger who published commentary critical of the government under a pseudonym. To protect his identity, he created a new email account for every article he sent, discussing them with with Karayev over Skype. Rasulov was arrested in 2013 and is now serving an 8-year-prison sentence for subversion. Karayev believes Rasulov was undone by surveillance. (Tulkin Karayev via AP)



This undated photo provided by exiled Uzbek activist Tulkin Karayev shows dissident Kudrat Rasulov, a blogger who published commentary critical of the government under a pseudonym. To protect his identity, he created a new email account for every article he sent, discussing them with with Karayev over Skype. Rasulov was arrested in 2013 and is now serving an 8-year-prison sentence for subversion. Karayev believes Rasulov was undone by surveillance. (Tulkin Karayev via AP)



Edin Omanovic, a research officer at Privacy International, poses for a photo at the company's offices in London on Wednesday, July 27, 2016. The advocacy group works to expose companies that enable surveillance that it says erodes people's privacy. "There is just so little reliable data on this," Omanovic said of the prevalence of off-the-shelf state surveillance tools. (AP Photo/Matt Dunham)



Edin Omanovic, a research officer at Privacy International, poses for a photo at the company's offices in London on Wednesday, July 27, 2016. The advocacy group works to expose companies that enable surveillance that it says erodes people's privacy. "There is just so little reliable data on this," Omanovic said of the prevalence of off-the-shelf state surveillance tools. (AP Photo/Matt Dunham)



In this Saturday, Feb. 14, 2015 file photo, former U.S. National Security Agency contractor Edward Snowden appears via live video from Moscow at an event in Honolulu. Documents on U.S. surveillance programs released in 2013 by Snowden showed how Washington and its allies were collecting the phone records of millions of Americans, few suspected of crimes. Even after some reforms, privacy advocates say there is still much to be done in the United States and abroad to rein in Big Brother. (AP Photo/Marco Garcia, File)

More information: Documents about the Peru program:
bit.ly/2awHVE0

© 2016 The Associated Press. All rights reserved.

Citation: Snapping up cheap spy tools, nations 'monitoring everyone' (2016, August 2) retrieved 25 April 2024 from <https://phys.org/news/2016-08-snapping-cheap-spy-tools-nations.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.